스머프 공격에 사용되는 ICMP ECHO 메시지 조각화의 취약성

민재원*, 한선희*, 조신영*, 정성민*, 정태명**
성균관대학교 전자전기컴퓨터공학과 *
성균관대학교 정보통신공학부 **
e-mail : {jwmin, shhan, sycho, smjung}@imtl.skku.ac.kr*, tmchung@ece.skku.ac.kr**

Vulnerability of fragmenting ICMP ECHO messages used in Smurf Attacks

Jae-Won Min*, Sun-Hee Han*, Shin-Young Cho*, Sung-Min Jung*, Tai-Myoung Chung**
Dept. Electrical and Computer Engineering, Sungkyunkwan Univ. *
School of Information Communication Engineering, Sungkyunkwan Univ. **

요 약

Denial of Service (DoS) 공격은 현재 심각한 국가적 보안 문제로 떠오르고 있다. DoS 란, 많은 양의 네트워크 트래픽을 발생시켜 속도를 매우 느리게 만들거나, 가용 자원을 고갈시켜 사용자에게 서비스를 정상적으로 제공하지 못하도록 만드는 공격이다. 그 중에서 Distributed Denial of Service (DDoS)는 네트워크에 분산된 컴퓨터들을 감염시켜 공격에 사용하기 때문에 더 위험하다. DDoS 종류 중 한가지인 Smurf Attack 은 ICMP ECHO 와 IP 브로드캐스트를 이용하여 많은 양의 트래픽을 발생시킨다. 본 논문에서는 Smurf Attack 에 쓰이는 ICMP ECHO REQUEST 패킷을 조각화시켜서 전송할 시, 피해자에게 전송되는 패킷의 숫자가 기존 방법보다 증가하고 피해자 컴퓨터의 IP 스택에서 발생하는 취약점을 도출하고 그로 인한 피해를 분석하였다. 끝으로 ICMP ECHO 패킷의 조각화를 방지하기 위한 방안을 제시하였다.

1. 서론

컴퓨터가 발전하면서 공격 또한 단순한 전화 조작에서 개인 정보 탈취 등으로 발전하였다. 공격자는 주로 시스템에 직접 침입을 해서 정보를 훔치거나 시스템을 훼손하였지만 Denial of Service 공격은 기존 방법과 추구하는 목적이 다르다. Denial of Service (DoS) 공격의 목적은 대상 컴퓨터의 권한을 탈취하여 피해를 입히는 것이 아니라 사용자가 대상 컴퓨터의 서비스를 이용하지 못하게 방해를 하는 것이다. 이 같은 목적을 달성하기 위해서 다량의 패킷을 전송해서 네트워크 대역폭을 포화시켜 일반 사용자의 접속을 방해하거나, 또는 공격 대상 컴퓨터의 자원을 고갈시켜 올바른 서비스를 제공 못하게 막는다[1].

그 중에서도 Distributed Denial of Service (DDoS) 공격은 여러 대의 컴퓨터가 동시에 하나의 공격 대상에게 DoS 공격을 하는 방법이다. 공격자는 공격에 사용될 컴퓨터들을 감염시키고 이들을 이용하여 공격을 수행한다. 공격자에 의해 감염된 컴퓨터들은 공격자의 명령대로 행동하기 때문에 흔히 좀비 PC 라고 칭한다. DDoS 는 여러 대의 컴퓨터가 공격에 참여하기 때문에 기존의 DoS 공격보다 피해는 더욱 크다.

많은 양의 자원이나 네트워크 대역폭을 가지고 있으면 DDoS 공격으로부터 안전하다고 생각할 수 있다. 하지만 거대한 기업의 서버 컴퓨터라고 해서 DDoS 공격으로부터 안전한 것은 아니다. 2000 년 2 월 27 일에는 Yahoo.com 이 DDoS 공격을 당했다. Yahoo.com 은 공격자 개인보다 훨씬 큰 컴퓨터 자원과 대역폭을 가지고 있었지만 분산된 여러 좀비 PC 들의 동시다발적인 공격으로 인하여 큰 손해를 입었다. 비슷한 사건으로 CNN, E-BAY, Amazon 도 DDoS 공격을 경험했다[4].

DDoS 사건이 계속 빈번하게 발생을 하면서 대책을 연구해 왔지만, DDoS 는 시간이 지날수록 더욱더 정교해지고 탐지가 어려워지고 있다. 뿐만 아니라, 특정 기업을 공격하는 것에서 공격 범위를 국가 수준으로 넓혀가고 있다. 최근 우리나라에서 발생한 7.7 DDoS 와 3.4 DDoS 공격을 예로 들 수 있겠다. 7.7 DDoS 공격은 미국의 백악관, 한국의 청와대 등 주요 사이트에 대한 공격이 약 4 일간 지속되었고 국정원과 방송통신위원회의 늦은 대응으로 국내 여러 사이트가 접속이 마비되었다. 3.4 DDoS 공격은 7.7 DDoS 공격보다 발전된 형태로, 백신 업데이트를 막고 공격에 사용된 좀비 PC 들은 하드드라이브가 파괴되도록 설계되었다. 비교적 피해는 적었지만, 여전히 공격의 근원은 파악하지 못한 상태로 남아있다. Arbor Network 의 조사에 따르면, DDoS 공격의 스케일은 2001 년부터 점점 커지고 있으며, 2008 년에 기록된 최대의 DDoS 공격 트래픽은 초당 40 gigabits 였고, 이는 2007 년 기록된 초당 24 gigabits 를 훨씬 압도하는 수치이다[4].

본 논문에서는 DDoS 공격의 한 종류인 Smurf Attack 의 동작 방식과 ICMP ECHO 패킷이 가지는 취약점을 설명하고, 그 취약점을 제거하기 위해 IP 와 ICMP 프로토콜에서 구현할 수 있는 해결책을 제시한다.

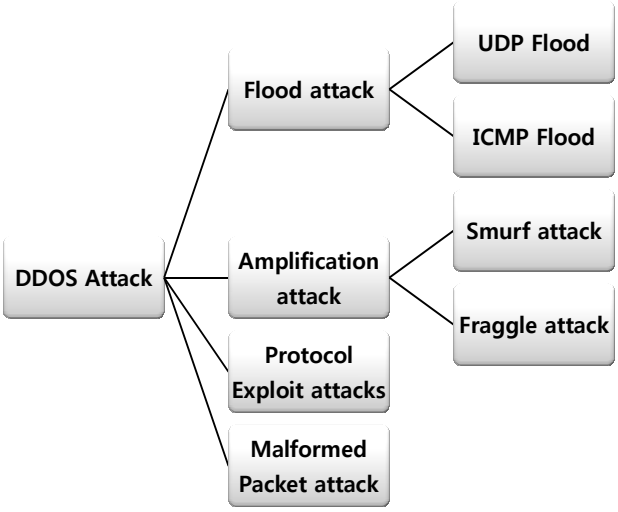
2 장 관련연구에서는 DDoS 의 종류에 대해서 설명

을 하고, 3 장 본론은 Smurf Attack 에 사용되는 ICMP ECHO 메시지가 악용될 수 있는 방법과 발생할 수 있는 피해에 대해서 서술한다. 이와 같은 피해를 방지하기 위한 몇 가지 대책을 4 장에서 설명하고 5 장으로 결론을 맺는다.

2. 관련 연구

2.1 DDoS 의 종류

DDoS 는 여러 가지 기준으로 나눌 수 있다. 본 장에서는 악용되는 취약점을 기준으로 (그림 1)과 같이 분류 하였다[1].



(그림 1) DDoS 공격의 종류

각 공격에 따른 특징은 <표 1> 과 같다.

<표 1> DDoS 공격의 특징

공격	특징
Flood	감염된 좀비 PC 를 통해서 다량의 IP 트래픽을 발생
Amplification	브로드캐스트 IP 주소라는 취약점을 사용하여 네트워크 트래픽을 증가
Protocol Exploit	특정 프로토콜의 설계적 결함을 찾아서 그 것을 악용
Malformed Packet	악의적으로 가공된 패킷을 전송함으로써 시스템의 오작동을 유발

Flood Attack 은 ICMP Flood 와 UDP Flood 로 나뉜다. 각각 ICMP 패킷과 UDP 패킷을 이용해서 네트워크 대역폭을 포화시킨다.

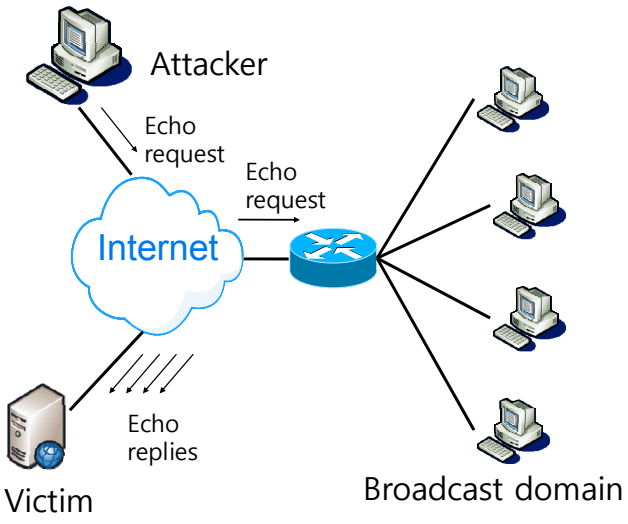
Smurf Attack 과 Fraggle Attack 은 Amplification Attack 의 대표적인 종류이다. 두 가지 공격이 서로 다른 점은, Smurf Attack 은 ICMP ECHO 패킷을 악용하고, Fraggle Attack 은 UDP 패킷을 사용한다는 점이다.

이와 같은 분류 이외에도 DDoS 공격의 구조에 따라서도 나눌 수 있다. 크게 Agent Handler 모델과 IRC 모델이 있다. Agent Handler 모델은 감염된 좀비 PC 또는 Agent 와 Handler 라는 시스템들을 통해서 공격을 위한 통신을 하는 구조이고 IRC 모델은 IRC 채널을 통해서 통신을 한다.

DDoS 에 대한 방어는 하나의 통일된 방법론이 존재하는 것이 아닌, 각각의 공격 종류에 대한 임시 방편적인 방식으로 이루어졌다. 따라서, 새로운 DDoS 공격을 받게 되면 피해를 막을 수가 없다. 본 논문에서는 Smurf Attack 이 사용하는 ICMP ECHO 메시지의 취약성을 제시하면서 현재 인터넷이 DDoS 공격으로부터 자유롭지 않다는 것을 설명한다.

2.2 Smurf Attack

Smurf Attack 은 DDOS 공격의 종류 중에서 Amplification Attack 에 속한다. Amplification Attack 은 공격자가 한 네트워크의 브로드캐스트 주소로 source IP 주소가 스푸핑된 ICMP ECHO REQUEST 패킷을 전송하고 패킷을 받은 네트워크의 다량의 컴퓨터들은 모두 ICMP ECHO REPLY 패킷을 source IP 로 전송한다. 스푸핑된 컴퓨터는 수많은 ICMP ECHO REPLY 패킷을 받게 되고 대역폭이 포화되어 정상적인 서비스를 제공하지 못하는 상태가 된다. 이 공격에서 사용되는 브로드캐스트 도메인을 reflector 또는 amplifier 라고 부른다. 이러한 reflector 또는 amplifier 를 여러 개 사용함으로써 더 많은 패킷을 생성할 수 있다.



(그림 2) Smurf Attack

(그림 2)는 Smurf Attack 의 과정을 설명하고 있다. 공격자가 브로드캐스트 도메인에 ICMP ECHO REQUEST 를 보내고 ICMP ECHO REPLY 가 라우터를 통해서 피해자에게 전송이 된다. 패킷의 IP 주소가 스푸핑 되었기 때문에 피해자는 공격자의 IP 주소를 알 수 있는 방법이 없다.

2.3 Smurf Attack 의 심각성

Smurf Attack 은 단시간에 다량의 패킷을 생성할 수가 있어서 매우 위험하다. <표 2>는 네트워크 종류에 따라서 공격에 얼마나 취약한지 설명하고 있다. <표 2>에 따르면, 증폭이 일어난 후에 트래픽이 3.66 Gbps 까지도 올라갈 수 있는 것을 알 수가 있고, 따라서 네트워크 대역폭을 쉽게 포화시킬 수 있다는 것을 보여주고 있다[2].

<표 2> 네트워크 종류에 따른 취약성

Type of compromised IP networks	Attack traffic load before amplification	# of amplifier networks	Attack traffic load after amplification	Type of network link vulnerable
Class C	56 kbps	1	14.28Mbps	T1, T3
Class C	56 kbps	4	57 Mbps	T3, OC-1
Class C	T1 line	2	765 Mbps	OC-12
Class B	56 kbps	1	3.66 Gbps	OC-48

Smurf Attack 을 막기 위한 여러 가지 방법들이 제안되어왔다. 한가지 예로 Windows XP Service Pack2 Security Software 는 Smurf Attack 등 ICMP 기반의 공격을 막기 위해서 모든 ICMP 메시지에 응답하지 않는다. ICMP 메시지를 받아들이지 않음으로써 문제가 해결되는 것처럼 보이지만 컴퓨터의 CPU 사용량이 계속 증가하기 때문에 여전히 공격에 취약하다. 연구에 따르면, Windows XP Service Pack2 Security Software 를 설치하지 않은 컴퓨터가 오히려 더 공격을 받았을 때의 CPU 사용량 증가율이 낮다[3].

네트워크 관리자는 라우터 설정을 하여 ICMP ECHO 패킷이 IP 브로드캐스트 주소로 전달되지 않게 필터링을 하기도 한다. 하지만 여전히 인터넷 상에는 ICMP 패킷을 통과시키는 네트워크가 존재하고, 공격자들은 프로그램을 통해 증폭기로 사용할 수 있는 네트워크를 검색해 이들을 악용 한다. 증폭기를 찾아내는 것에 성공을 한다면, 피해자가 연결되어 있는 라우터가 ICMP 트래픽을 필터링 한다고 해도 라우터가 DDoS 공격을 받을 수가 있다. Smurf Amplifier Registry (SAR)은 증폭기로 악용 가능한 네트워크 주소들을 데이터베이스에 저장을 하고 있는데, 아직도 취약한 네트워크가 존재한다는 것을 알 수가 있다[5].

최근에는 Amplification Attack 이 계속 지능화 되고 있다. 패킷 증폭 매커니즘을 ICMP ECHO 패킷에 한정하지 않고, DNS 서버를 악용하는 등 다양한 방법으로 발달하고 있다. 앞에서 설명했듯이, 이러한 새로운 공격 방법은 기존의 방어책으로 피해를 막을 수 없다.

3. ICMP ECHO 패킷의 취약성

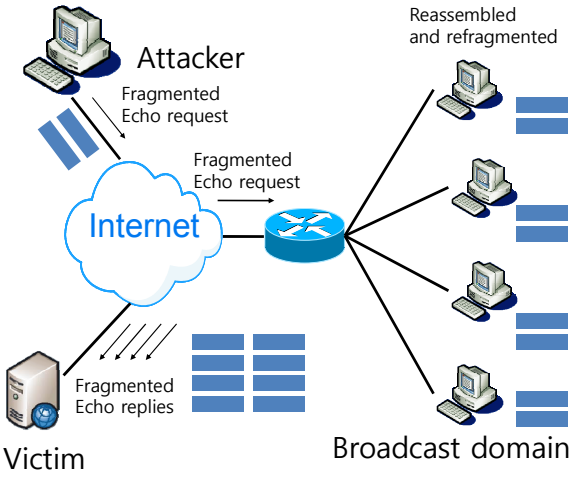
3.1 Fragmenting Smurf Attack Packets

Smurf Attack 에서 사용되는 ICMP ECHO 패킷의 특징은 REQUEST 패킷의 데이터 부분을 REPLY 패킷이 복사해서 전송한다는 것이다. 이것은 REPLY 패킷과 해당되는 REQUEST 패킷을 대응시키기 위해서이다. <표 3>는 ICMP 프로토콜의 ECHO 패킷의 포맷을 나타내고 있다. Optional Data 영역에 데이터를 채워 넣는다.

<표 3> ICMP ECHO format

TYPE(0)	CODE(0)	CHECKSUM
IDENTIFIER		SEQUENCE NUMBER
OPTIONAL DATA		
…		

보통 ICMP data 부분에는 TCP 헤더의 8 bytes 가 저장되고 전체 ICMP 패킷은 IP 패킷에 캡슐화 되어 전송된다. 만약 이 데이터 부분을 비정상적으로 크기를 증가시킨다면, 공격자의 IP 스택에서 패킷을 조각화 시켜 전송을 하게 된다. 이 조작된 패킷은 증폭기로 전송이 되고 증폭기 컴퓨터들의 IP 스택에서는 패킷의 조각들이 모두 수신 될 때까지 기다리고 재조합을 한다. 그리고 ICMP ECHO REPLY 패킷을 보낼 때 데이터 부분을 동일하게 전송을 해야 되기 때문에 역시 조각화가 발생한다. 이와 같은 과정을 (그림 3)으로 표현하였다.



(그림 3) Fragmenting Smurf Attack

조각화 방법은 공격자가 ICMP ECHO REQUEST 패킷을 순차적으로 보내는 것과는 차이점이 있다. 순차적으로 전송을 하면, 증폭하는 과정을 반복하는 것에 불과하다. 만약 브로드캐스트 도메인에 있는 컴퓨터의 숫자를 n 이라고 한다면, ICMP ECHO REQUEST 패킷 한 개당 생성되는 패킷의 개수는 n 개이다. 만약 REQUEST 패킷을 두 개의 조각으로 나눈다면, REQUEST 패킷 한 개당 생성되는 REPLY 패킷의 숫자는 2n 개이다.

3.2 Fragmentation 의 심각성

기존의 Smurf Attack 공격보다, ICMP ECHO 메시지 한 개당 생성되는 패킷의 숫자가 조각화 정도에 따라 배수로 늘어나기 때문에 보다 더 빠르게 네트워크 대역폭을 포화시킬 수 있다. 뿐만 아니라, 패킷의 크기

가 클수록 라우팅 과정에서 MTU 가 작은 네트워크를 만나 추가적으로 조각화가 발생할 경우도 생길 수 있기 때문에 패킷의 숫자가 증가하게 된다.

Smurf Attack 을 할 때 조각화를 발생시켜서 얻을 수 있는 또 다른 공격의 심각성은, IP 스택이 조각화된 패킷을 수신했을 때 하는 행동에 있다. IP 스택은 IP 패킷의 조각들을 재조합 하여 transport layer 에 넘겨주기 위해 재조합 테이블에 엔트리를 추가하고 링크드 리스트 형태로 패킷을 메모리에 저장해둔다. 만약 모든 조각들이 도착하면 링크드 리스트를 해제하고 상위 계층으로 재조합을 해서 보낸다. 기존 Smurf Attack 은 패킷이 조각화 되지 않았기 때문에 링크드 리스트를 만들지 않는다. 반면에, 피해자가 수많은 ICMP ECHO REPLY 패킷의 조각들을 수신하게 되면, 각각의 패킷마다 링크드 리스트를 유지하고 있어야 되기 때문에 엄청난 리소스를 소모하게 되고, 또한 재조합 테이블을 검색하는데 걸리는 오버헤드 때문에 서비스 불능상태에 도달하는 시간이 단축된다.

4. 제안하는 해결책

본 논문에서는 조각화 공격을 막기 위한 방어책을 두 가지 제시한다. 첫 번째는 ICMP ECHO REQUEST 를 받았을 때 커널의 ICMP 모듈 자체에서 ICMP ECHO REPLY 의 사이즈를 제한하는 방법이다. 따라서 조각화된 ICMP ECHO REQUEST 을 수신해도 재조합을 해서 REPLY 하는 과정에서 에러가 발생하게 된다. 보통 ICMP 프로토콜을 사용할 때 데이터 영역에 많은 정보를 저장하지 않기 때문에 사이즈를 제한하는 방법은 합리적이다. 예를 들어 ping 이라는 유틸리티는 ICMP ECHO 패킷의 데이터 영역에 타임스탬프 값들을 저장하는데, 타임스탬프 값은 많은 양의 공간을 차지하지 않는다.

또 다른 방법은 IP 스택에서 ICMP 패킷의 조각화를 막는 방법이다. IP 패킷은 캡슐화되는 데이터의 프로토콜 정보를 헤더에 저장한다. ICMP 프로토콜의 값은 1 이다. 따라서 IP 스택에서 IP 패킷을 조각화 하기 전에 캡슐화된 페이로드가 ICMP 패킷인지 검사를 하고, 만약 ICMP 패킷이라면, 조각화를 하지 않는다. 이 방법은, ICMP ECHO REQUEST 와 REPLY 패킷의 조각화를 방지할 수 있다.

5. 결론

본 논문에서는 기존 Smurf Attack 을 분석하고 공격에 사용되는 ICMP ECHO 패킷이 가지는 취약점을 설명했다. ICMP 프로토콜이 ECHO REQUEST 패킷의 데이터 영역을 똑같이 복사를 해서 ECHO REPLY 를 한다는 점을 악용하면 기존 Smurf Attack 보다 더 큰 피해를 발생시킬 수 있다.

이러한 ICMP ECHO REPLY 패킷의 취약성을 방지하기 위해서 두 가지 해결책을 제시했다. 공격 방법은 계속 진화하고 있기 때문에 방어책 또한 계속 발전한다면, 컴퓨터들이 보다 더 안전하게 정상적인 서비스를 제공할 수 있을 것이다.

따라서, 추후 연구의 방향은 특정 공격에 대한 방어가 아니라, 모든 DDoS 공격으로부터 시스템을 지킬 수 있는 방어 인프라 구축이 되어야 할 것이다.

ACKNOWLEDGMENT

본 논문은 중소기업청에서 지원하는 2010 년도 산학연공동기술개발사업(No. 00044301)의 연구수행으로 인한 결과물임을 밝힙니다.

참고문헌

[1] Christos Douligeris, Aikaterini Mitrokotsa, “DDOS attacks and defense mechanisms: classification and state-of-the-art”, Computer Networks 44, pp.643-666, 2004.

[2] Sanjeev Kumar, “Smurf-based Distributed Denial of Service (DdoS) Attack Amplification in Internet”, ICIMP , pp.25, 2007.

[3] S.Kumar, M.Azad, O.Gomez, R.Valdez, “Can Microsoft’s Service Pack2(SP2) Security Software Prevent SMURF Attacks?” Proceedings of AICT/ICIW, 2006.

[4] Arun Raj Kumar, P. S. Selvakumar, “Distributed Denial-of-Service (DDoS) Threat in Collaborative Environment- A Survey on DDoS Attack Tools and Traceback Mechanisms” IACC, 2009.

[5]” Smurf Amplifier Registry (SAR)”, http://www.powertech.no/smurf, Mar. 2011.